Google Cloud

Google Cloud Whitepaper

June 2023

Insights into the U.S. Telecommunications Industry

Disclaimer

This whitepaper applies to Google Cloud products described in the Google Cloud Services Summary. The content contained herein is correct as of June 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Telecommunications is perhaps the most significant engine of world economic growth. Telecoms have powered social change and business expansion for almost 200 years, from telegraphs at the dawn of the Industrial Revolution, to today's mobile apps, video, and data services. It's easy to see why: Communications Service Providers (CSPs), as they are known today, connect people and their inventions, enabling new markets and innovations.

The industry, however, finds itself in the midst of epic disruption - facing low single-digit revenue growth[1], increasing CAPEX investments and demand on the network, and challenges in customer experience. Accordingly, CSP leaders around the world are looking at innovative ways to unlock new revenue streams, transform the end-to-end customer experience, handle explosive usage, effectively manage increasingly complex systems, unlock the full potential of their data, and deliver on sustainability objectives.

Underpinning these focus areas, CSPs globally are focused on ensuring they operate their critical infrastructure in line with ever-evolving regulatory, security, data privacy, and sovereignty requirements. As CSPs accelerate their digital transformation journeys towards long-term growth - powered by cloud technology - there is a need to understand both the implications of these regulations for cloud and how the cloud can help CSPs to address these challenges.

This paper provides:

- An overview of the security-related regulations, guidelines, and standards that apply to CSPs within the context of the United States
- Insight into the key themes and principles that emerge from the regulations
- Guidance on how Google Cloud can help CSPs meet their regulatory requirements

Regulatory themes

Within the U.S., telecom networks have a critical role in supporting economic prosperity and national security. CSPs are also trusted with large amounts of sensitive customer information. Therefore, CSPs and the telecom networks they operate are subject to many security and privacy-related regulations. In the context of the U.S., this includes global security standards and state and federal-level regulations and guidelines.

A survey of specific regulations affecting CSPs is included in the Appendix. This section summarizes the main themes emerging from these regulations and how Google Cloud can help.

Foundational security

CSPs are high-profile targets for cybersecurity attacks and require protection against cybersecurity risks, including state-level and state-sponsored attacks, insider threats, organized crime, industrial espionage, and sabotage. Increasing cybersecurity concerns have led to

[1] TM Forum, September 2022

governments and organizations to work together to shape cybersecurity requirements and frameworks. This includes Global Standards, such as ISO 27001 and ISO 27017, and the Cloud Controls Matrix from the Cloud Security Alliance.

Within the U.S., the Communications Sector has been identified as Critical Infrastructure, and the Department of Homeland Security has created a Communications Sector-Specific Plan.

Additionally, the Cybersecurity Infrastructure & Security Agency (CISA) and the National Security Agency (NSA) have jointly published cybersecurity guidance for 5G Cloud infrastructure.

These security regulations and guidelines identify many specific security measures and best practices across domains, such as physical security, network security, identity and access management, security incident management, and personnel security.

How we help: Google Cloud has comprehensive and in-depth security controls that we deploy to help protect your data, summarized in this security overview whitepaper. Other whitepapers detail our security practices in specific areas, such as encryption at rest, encryption in transit, and infrastructure security. Google Cloud also publishes guidance on security best practices, use cases, and blueprints.

Google Cloud's security, third-party audits, and certifications help support your compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Cloud undergoes several independent third-party audits regularly to provide this assurance. Some of the key international standards we are audited against include:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- CSA Star Cloud Controls Matrix
- AICPA SOC 2 and SOC 3 reports

At the U.S. national level, Google Cloud is authorized by FedRAMP to provide Cloud services to the U.S. Federal Government. We are compliant with NIST 800-53, which specifies security and privacy controls required for federal government and critical infrastructure (including the Communications Sector).

Google Cloud security capabilities are also well aligned with the NSA/CISA Cybersecurity Guidance for 5G Cloud Infrastructure, including support for the following features:

- Identity & Access Management and Multi-Factor Authentication
- Audit Logging of all access requests and admin activity
- Use of a security-hardened Operating System for Container Platforms.
- Automated patching of Operating System and Kubernetes
- Secure CI/CD and container attestation

- Scanning containers for Security Vulnerabilities
- Scanning deployments for abnormal behaviors and events.
- Default firewall rules and support for Kubernetes network policies
- Use of Service Mesh technologies to protect node-to-node traffic
- Using analytics to process cloud logs and other telemetry, to detect known threats and identify anomalies
- Kubernetes native security controls
- Confidential Computing (Trusted Execution Environment)
- Secure Boot and Trusted Platform Modules
- Encryption of data-in-transit
- Encryption of data-at-rest
- Cloud-based Hardware Security Modules
- Customer control of Encryption Keys (including key rotation)

Data privacy and communications confidentiality

CSPs are entrusted with large volumes of sensitive customer data, including communications data, personally identifiable information (PII), and payment card information (PCI). With some U.S. CSPs providing services to over 100M customers[2][3][4],the consequences of a potential data breach are severe.

Protecting customer data privacy and confidentiality of communications are fundamental requirements for telecom operators. Within the U.S., this means ensuring compliance with the Federal Communication Commission's Customer Proprietary Network Information (CPNI) requirements as per Section 222 of the Communications Act of 1934, and data privacy requirements such as California Consumer Privacy Act (CCPA) and similar regulations in other states. Compliance with Payment Card Industry Data Security Standards (PCI DSS) is also required.

How we help: Google Cloud's trust principles provide a starting point for our approach to data privacy. The data you put into Google Cloud services is yours. We do not scan it for advertisements, and we do not sell it to third parties. The Cloud Data Processing Addendum for Google Cloud describes our commitment to protecting your data. That document states that we will not process data for any purpose other than to meet our contractual obligations. Google Cloud is also compliant with international standards on data privacy, such as:

- ISO 27018 (Cloud Privacy)
- ISO 27701 (Privacy - Data Processor)

[2] Telegeography, 2023
[3] T-Mobile news, 2023
[4] Telegeography, 2023

- PCI DSS

From a U.S. perspective, Google Cloud complies with NIST 800-53, which specifies security and privacy controls required for federal government and critical infrastructure (including the Communications Sector).

Further information is available from Google Cloud's Privacy Resource Center and Google's whitepaper on trusting your data with Google Cloud.

Data residency

As data privacy laws proliferate within the U.S., a growing demand exists for CSPs to implement data residency controls for sensitive customer data. When moving to a cloud environment, CSPs may need to validate and control where their data resides. In some cases, this may include the need to control the locations in which they provide technical support.

How we help: The majority of Google's Public Cloud services can be configured for data residency to control the physical location of customer data. Google Cloud has regions in Oregon, Salt Lake City, Las Vegas, Los Angeles, Iowa, Columbus, North Virginia, South Carolina, and Dallas - providing customers with many options for data localization within the U.S..

Remote access to data (for reasons such as technical support) can be considered a data transfer. To help customers address this concern, customers can limit Google Cloud administrator access to their data via Access Approval and monitor via Access Transparency. For U.S.-based customers, Google Cloud offers additional data residency support (including U.S.-based technical support) via Assured Workloads.

Operational requirements

Should the availability of public communication services be impacted by a security incident, a widespread disruption could occur, including the possible inability to contact emergency services and the consequences could be measured in human lives lost. CSPs could also face fines, reputational damage, and loss of business.

CSPs must design for high availability and plan for business continuity and disaster recovery. CSPs also require oversight of software changes that could impact their services to ensure that software deliverables do not compromise service availability or introduce security vulnerabilities.

How we help: CSPs are responsible for ensuring they are designing for high availability (as well as security) when planning cloud solutions. Google Cloud publishes architecture

guidelines to assist with this. Google Cloud also supports customers with Backup and Disaster Recovery solutions. CSPs can use these solutions to design, build, and validate robust disaster recovery patterns that meet their specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

To complement this, Google Cloud also has comprehensive internal plans and systems for its business continuity (refer to ISO 22301).

Google Cloud also offers customers the choice of manual or automated software updates, with the flexibility to control software update approvals and scheduling. Refer to OS Patch Management for an example of this flexibility.

Google Cloud security solutions

In addition to the security features and regulatory compliance described above, Google Cloud offers many Security solutions for a more comprehensive and holistic approach to security.

When migrating to the cloud, CSPs may not initially have the expertise to decide which security capabilities they need. Our Security solutions help customers identify those needs and rapidly roll out relevant security functionality based on common blueprints and established best practices.

Security Foundations solution

As a starting point for customers who need clarification on their security needs, the Security Foundations solution includes a set of recommended products and security capabilities to help CSPs achieve a strong security posture within their Google Cloud environment.

This solution is based on the Security Foundations whitepaper and aligns with Google Cloud's security best practices.

Security and Resilience Framework (SRF) solution

Google Cloud can also support CSPs to carry out a thorough review of their security practices.

The Security and Resilience Framework helps customers to establish or refresh their security program, founded on a risk-based assessment of the entire cybersecurity lifecycle (identify, protect, detect, respond, recover), utilizing established industry frameworks.

The Discovery Platform supports the assessment and includes security maturity assessments across multiple domains. Google Cloud will provide a tailored set of recommendations around security best practices and recommended Google Cloud security products and solutions.

Web App and API Protection (WAAP) solution

The Web App and API Protection solution provides capabilities that protect applications, websites, and public APIs from internet-based threats, including DDOS, fraud, and botnet attacks.

This solution is relevant for all CSPs since DDOS attackers commonly target CSP infrastructure and systems, and CSPs are increasingly adopting APIs that expose their capabilities.

The WAAP solution includes the following products:

- Cloud Armor
- reCAPTCHA Enterprise
- Apigee API Management

Risk and Compliance as Code (RCaC) solution

Achieving, maintaining, and demonstrating compliance with relevant security regulations is critical for all CSPs. Google Cloud's Risk and Compliance as Code (RCaC) solution combines several capabilities to help meet this challenge.

By adopting this solution, CSPs can prevent non-compliance by asserting infrastructure and policies as code for easy onboarding to Google Cloud and establish secure guardrails from the get-go via security blueprints and Assured Workloads. Additionally, they can detect non-compliance via Security Command Center, notify stakeholders when offending infrastructure is identified, and reduce risk with intelligent automation, control mapping, and continuous assessments. Finally, once on Google Cloud, CSPs can leverage Risk Manager to continuously evaluate risk and utilize our Risk Protection Program to qualify for cyber insurance.

Autonomic Security Operations (ASO) solution

Google Cloud's Autonomic Security Operations solution helps CSPs withstand security attacks through an adaptive, agile, and highly automated approach to threat management.

This solution is relevant for CSPs that are interested in transforming their existing Security Operations Centre (SOC) or Security Incident and Event Management (SIEM) by increasing scale, automation, and the use of machine learning (ML) to keep up with a high volume of security incident data and deliver effective threat intelligence and incident response.

By leveraging the power of Chronicle and Mandiant, customers can transform their security operations and achieve a 10X increase in productivity, visibility, and speed. For more information, refer to our Autonomic Security Operations whitepaper.

Software Delivery Shield solution

Google Cloud's Software Delivery Shield offers a fully managed, end-to-end solution that enhances software supply chain security across the entire software development life cycle from development, supply, and CI/CD to runtimes.

As CSPs move towards software-based networks and adopt cloud-native applications and modern software development processes (including automated testing, deployment, and faster and more numerous deployments), new security challenges emerge. A modern software development and deployment pipeline with secure and automated DevOps processes has become more critical than ever.

Using this solution, CSPs can:

- Enhance application security in development environments
- Improve the security of application images and dependencies
- Strengthen the security of CI/CD pipelines
- Protect running applications
- Enforce trust-based security policies throughout SDLC.

Conclusion

With the exponential proliferation of technology to deliver products, services, and payments comes the need for an underlying infrastructure that can manage billions of transactions across the network with little to no downtime. Telecommunications companies are continuously working on solutions that can provide a platform that offers a seamless experience for consumers while working within the boundaries of the ever-changing legislative and industry landscape. Consequently, these companies are looking to partner with organizations whose products are scalable and secure, reliable, fault-tolerant, capable of low-latency delivery and while meeting their customer and regulatory requirements.

Google has a track record of delivering on every front mentioned above, which is why several major U.S. providers continue to partner with Google as they introduce their latest network and technological advancements to the market. Whether it be operational resilience, disaster recovery capabilities, encryption of data in rest and in motion, or meeting privacy needs, Google is committed to keeping in step with the continuously evolving needs of their customers in the telecommunications industry.

Appendix A: Regulations and Standards Impacting the Telecom Industry

This appendix contains a survey of relevant global, federal and state-level security standards, regulations, and guidelines for U.S. CSPs. This whitepaper is not intended to represent all of the compliance enablement features Google Cloud offers its customers and may not include a summary of all applicable laws.

Global Security Standards

The following global standards on Information Security are not specific to CSPs but are widely accepted as a baseline for good security practices and provide a way to measure organizational compliance to internationally recognized security policies.

Google Cloud supports compliance with the following standards:

- ISO 27001 outlines and provides the requirements for an information security management system, specifies a set of best practices and details the security controls that can help manage information risks
- ISO 27017 provides guidelines for information security controls applicable to the provision and use of cloud services
- ISO 27018 relates to one of the most critical components of cloud privacy - the protection of personally identifiable information (PII)
- AICPA SOC2 is based on the Statement of Standards for Attestation Engagements No.18 (SSAE 18).
- CSA SOC2+ demonstrates compliance with the Cloud Security Alliance Cloud Controls Matrix (CCM) - designed to help customers assess and select a Cloud Service Provider.

Refer to the Google Cloud Compliance Resource Center for more information on the above standards, plus many more.

Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) regulates CSPs in the U.S.

The FCC is an independent agency of the United States federal government that regulates communications by radio, television, wire, satellite, and cable across the United States. The FCC maintains jurisdiction over broadband access, fair competition, radio frequency use, broadcast television and radio, and access to public safety and homeland security related networks.

The primary law covering telecommunications service providers in the U.S. is the Communications Act of 1934, as amended (Communications Act).

The FCC publishes a compliance guide on **Customer Proprietary Network Information (CPNI),**

which details the steps required to comply with **section 222 of the Communications Act**, 47 U.S.C. § 222.

Section 222 states all telecommunications carriers and interconnected VoIP providers must take steps to protect CPNI (including to whom, where, and when calls were made) and to prevent unauthorized disclosure. Carriers must also complete the annual certification process demonstrating compliance.

In particular, Section 222 requires covered providers to:

- Safeguard CPNI
- Enforce controls for authorized access of CPNI
- Provide guidelines for the use of CPNI for marketing while respecting customer opt-in/opt-out approval
- Require training for employees with regard to the safe handling of CPNI
- Notify law enforcement and impacted customers of a breach of CPNI
- Notify customers of their right to restrict the use of CPNI
- Maintain certain records
- Annually certify compliance with the CPNI rules

Data Privacy laws

While there have been efforts in the past to protect individuals' data in the U.S., such protections were sector-specific and covered particular types of information. For instance, the HIPAA Privacy Rule applies to health information, and the Gramm-Leach-Bliley Act is targeted at protecting financial information.

With the passage of the **California Consumer Privacy Act** (CCPA) in 2018, U.S. lawmakers started to enforce broader consumer privacy protections (similar to EU GDPR and similar legislation adopted in many other nations).

Since CCPA was passed, additional states have been evaluating or passing similar legislation, for example:

- ColoPA (Colorado)
- CTDPA (Connecticut)
- UCPA (Utah)
- VCDPA (Virginia)

A federal-level law, the American Data Privacy & Protection Act, was proposed in2022 – but at the time of writing has not been passed into law.

EO 14028 and the White House National Cybersecurity Strategy 2023

EO 14208 is an executive order that strengthens cybersecurity measures at the federal level and directs the private sector to cooperate with federal government agencies on cybersecurity. It

charges multiple agencies, including NIST and CISA, to enhance cybersecurity through various initiatives, including:

- improving information sharing
- modernizing cybersecurity standards
- improve software supply chain security
- improving investigative and remediation capabilities

This effort is complemented by the National Cybersecurity Strategy. This document highlights the growing cybersecurity threats to U.S. national security interests, including attacks on critical infrastructure, ransomware attacks, and cyber-influence campaigns.

1. Defend Critical Infrastructure (including the establishment of cybersecurity regulations via NIST and CISA)
2. Disrupt & Dismantle Threat Actors
3. Shape Market Forces to Drive Security & Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships

Note that within the U.S., the Communications Sector has been identified as Critical Infrastructure, and there is a Communications Sector-Specific Plan created by the Department of Homeland Security.

NSA/CISA Security Guidance for 5G Cloud Infrastructures

CISA and the NSA (National Security Agency) have jointly published cybersecurity guidance for 5G Cloud infrastructure. The document is available in four parts:

- Part I - Prevent & Detect Lateral Movement
- Part II - Secure Isolate Network Resources
- Part III - Data Protection
- Part IV - Ensure Integrity of Cloud Infrastructure

Each document contains multiple specific technical recommendations. Google Cloud security capabilities are well-matched to this guidance. For further details, refer to the main part of this document.

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a U.S. government program that enables the adoption of cloud products and services while providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. To provide products and services to government agencies, a telecom provider needs to be **FedRAMP authorized** in accordance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, and FedRAMP policy based on NIST standards and guidelines. Providers must go through three phases to achieve authorization, which at a high level include:

1. **Preparation:** An optional (but highly recommended) readiness assessment and pre-authorization.

2. **Authorization:** A full security assessment performed by an accredited Third Party Assessment Organization and the agency authorization process where a cloud service provider works directly with the Agency sponsor who reviews the cloud service's security package. After completing a security assessment, the head of an Agency (or their designee) can grant an Authority to Operate (ATO). You can visit the FedRAMP Get Authorized page for more information on the authorization process.

3. **Continuous monitoring:** Depending on the impact the loss of confidentiality, integrity, and availability of data will have, providers are classified at low, medium, or high impact levels, which in turn informs the security controls they will need to satisfy.

How we help: For telecom leaders interested in validating Google's FedRAMP status, it is available on the government's website, FedRAMP Marketplace, and our FedRAMP compliance page.